

RESEARCH ETHICS

Legal and ethical considerations in processing patient-identifiable data without patient consent: lessons learnt from developing a disease register

Charlotte L Haynes, Gary A Cook, Michael A Jones

J Med Ethics 2007;33:302–307. doi: 10.1136/jme.2006.016907

The legal requirements and justifications for collecting patient-identifiable data without patient consent were examined. The impetus for this arose from legal and ethical issues raised during the development of a population-based disease register. Numerous commentaries and case studies have been discussing the impact of the Data Protection Act 1998 (DPA1998) and Caldicott principles of good practice on the uses of personal data. But uncertainty still remains about the legal requirements for processing patient-identifiable data without patient consent for research purposes. This is largely owing to ignorance, or misunderstandings of the implications of the common law duty of confidentiality and section 60 of the Health and Social Care Act 2001. The common law duty of confidentiality states that patient-identifiable data should not be provided to third parties, regardless of compliance with the DPA1998. It is an obligation derived from case law, and is open to interpretation. Compliance with section 60 ensures that collection of patient-identifiable data without patient consent is lawful despite the duty of confidentiality. Fears regarding the duty of confidentiality have resulted in a common misconception that section 60 must be complied with. Although this is not the case, section 60 support does provide the most secure basis in law for collecting such data. Using our own experience in developing a disease register as a backdrop, this article will clarify the procedures, risks and potential costs of applying for section 60 support.

In this paper we discuss the actions taken during the development of a disease register to ensure ethical and legal processing of patient-identifiable data. This paper provides researchers from English/Welsh organisations with a set of instructions to follow when processing patient-identifiable data without patient consent for medical purposes other than healthcare, such as medical research. The considerations do not apply to cases in which the data will be used to contact patients directly, nor when collecting data on sexually transmitted diseases, which are subject to a specific statutory duty of confidence.²

Why do we need patient-identifiable data?

Patient-identifiable data refer to any personal data that can be used directly or indirectly to identify an individual (eg, name or postcode). This also includes encrypted data if the solution for decryption is still in existence (eg, new National Health Service (NHS) number).³

The difficulties for epidemiological and health economics research if identifiable data are only accessible through informed consent have been highlighted in a number of articles.^{4–7} One concern is that updating, linking and validating data would be impossible without using some form(s) of patient-identifiable data,⁴ as is the case when developing disease registers. Another concern is that research conclusions would be flawed if patient identifiers—age, gender, ethnicity, geographical location and socioeconomic status (which may be derived from postcode data)—were not included in data analysis, as these are all potential confounders and effect modifiers.

Why not pursue informed consent?

From a practical perspective, obtaining informed consent may well be detrimental to case ascertainment. The process itself may result in a biased sample as groups such as the unemployed, severely ill and students are difficult to contact.^{8,9} The process of gaining informed consent from a large population may also be prohibitively costly in time and money.

Patient-identifiable data are critical in medical research and required for the developmental stages of disease registers. The problem is that pursuing informed consent for the use of such data is likely to result in a biased sample and is often prohibitively expensive. To get around this problem, some researchers believe that compliance with the Data Protection Act 1988 (DPA1998) is all that is required to meet regulations for processing (collecting, using and disclosing) patient-identifiable data without patient consent. However, this leaves projects at risk of breaching the common law duty of confidentiality. This can be overcome through gaining approval under section 60 of the Health and Social Care Act 2001.¹ The actual risk to researchers associated with the common law duty of confidentiality is, however, unclear and will be further elucidated upon in this paper.

See end of article for authors' affiliations

Correspondence to:
Dr C L Haynes,
Epidemiology, Stockport
NHS Foundation Trust,
Stepping Hill Hospital,
Stockport SK2 7JE, UK;
charlotte.haynes@
stockport-tr.nwest.nhs.uk

Received 31 March 2006
Revised 1 August 2006
Accepted 8 August 2006

Abbreviations: CVD, cardiovascular disease; DPA1998, Data Protection Act 1998; GP, general practitioner; HRA1998, Human Rights Act 1998; NHS, National Health Service; PIAG, Patient Information Advisory Group

Box 1 The Data Protection Act 1998, relevant schedules

Schedule 2: relevant paragraphs:

"5 The processing is necessary—
(d) for the exercise of any other functions of a public nature exercised in the public interest.

6(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject."

Schedule 3: relevant paragraphs:

8(1) "The processing is necessary for medical purposes and is undertaken by—

(a) a health professional (as defined in section 69 of the Act); or

(b) a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph 'medical purposes' includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services."

Justification for not pursuing informed consent

The issue as to whether informed consent should be sought is not clear cut, and is subject to ongoing ethical and legal debate.^{10–11} Some researchers have found that lack of consent does not indicate true refusal for data to be used, rather, it reflects factors such as time constraints, lack of interest, severity of illness, illiteracy and geographical mobility.^{8–9} Others have found that members of the public are concerned about the current data collection procedures, and are not happy for their data to be used in medical research and to populate disease registers.¹² From a legal perspective, there are three issues to consider when using patient-identifiable data without consent: the DPA1998, the law of confidentiality and the Human Rights Act 1998 (HRA1998).

THE LEGAL PERSPECTIVE Data Protection Act 1998

The implications of the DPA1998¹³ on processing patient-identifiable data without patient consent are well-rehearsed in the literature,^{4–7–14} and the majority of researchers are aware of their need to show compliance with the DPA1998. The DPA1998 establishes a series of data protection principles by which personal data must be processed, maintained and transferred. These principles are meant to ensure fair, lawful and proportionate use of data. The Act stipulates certain conditions that must be satisfied for the processing of personal data and for sensitive personal data to be lawful. "Personal data" refer to data, which alone, or in conjunction with other information in the possession of, or likely to come into the possession of the data controller, can identify a living individual. "Sensitive personal data" include information as to the physical or mental health or condition of the data subject.

To comply with the Act one must show that, in the case of sensitive personal data, at least one of the conditions in Schedule 2 and one of the conditions in Schedule 3 of the Act are met. In the absence of consent, the two conditions from Schedule 2 that would cover the creation and maintenance of a disease register are in paragraphs 5(d) and 6(1) of the Schedule

(box 1). The most relevant condition in Schedule 3 is in paragraph 8, which specifically covers medical research and preventive medicine (box 1), and clearly applies to a disease register.

There is a further hurdle in the Act, contained in the second data protection principle. This provides that personal data shall only be obtained for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with those purposes. It might be argued that when patients provide information for the purpose of their own treatment, it is then "incompatible" to use the data for research or public health monitoring. However, Section 33(2) provides that further processing of personal data for research purposes is not regarded as incompatible with the purposes for which they were obtained, provided that the data are not processed to support measures or decisions with respect to particular individuals, and that the data are not processed in such a way that substantial damage or distress is, or is likely to be, caused to any data subject.

The law of confidentiality

Compliance with the DPA1998 does not, however, negate the common law duty of confidentiality: when information of a confidential nature is disclosed to someone in confidence, as exemplified by the patient–doctor relationship, then the confidant (ie, doctor) normally has a duty not to disclose this information without the consent of the confider (ie, patient). The difficulty with interpreting the common law duty of confidentiality is that it is not codified in statute. It is an obligation derived from case law, and is open to interpretation: decisions are made on a case-by-case basis.^{1–15} There are, however, a number of defences to breaches of confidentiality. The most important defence is where disclosure would be in the public interest. There is good reason to believe that certain types of research are in the "public interest". For example, in the case *R versus Department of Health, ex parte Source Informatics*,¹⁶ there was an allegation of breach of confidentiality of patient records. The Court of Appeal suggested that the use of identifiable data for the purpose of audit, provided the use is "very strictly controlled", was acceptable because it could be defended as within the public interest and because the scope of the duty of confidentiality was restricted to accommodate such use. One drawback of relying on the public interest defence is that the concept of public interest is vague, and ultimately it is a matter for a court to determine.

Section 60 of the Health and Social Care Act 2001

Section 60 of the Health and Social Care Act 2001 now provides for the processing of patient-identifiable data despite the common law duty of confidentiality.¹⁷ The Act allows the secretary of state to make regulations permitting the processing of patient information for medical purposes that are considered necessary or appropriate in the interests of improving patient care, or in the public interest. Proposals for section 60 support are considered by the Patient Information Advisory Group (PIAG). Support will not be granted if it is deemed feasible to obtain patients' consent or anonymise the data. Section 60 support is a transitional measure to allow time for the introduction of policies to obtain consent and/or techniques for anonymising data.¹⁸ It is reviewed annually. Hence, once one decides to apply for section 60 support, one has to annually justify the use of patient-identifiable data without patient consent. Box 2 gives the broad criteria used to determine whether or not section 60 support should be granted, and are invaluable to those who decide to apply for section 60 support.

The decision to apply for section 60 support should not be taken lightly as it can be an awkward process¹⁹ and may result in being told that consent is in fact required.⁸ Importantly, one

Box 2 The Patient Information Advisory Group criteria for section 60 support for the use of patient-identifiable information without patient consent

Relevant acts and guidelines: The activity must be a medical purpose as defined in section 60 of the Health and Social Care Act 2001.

Provide clear evidence that your organisation is complying with the Data Protection Act 1998.

Provide clear evidence that you are following best practice in terms of confidentiality (eg, Caldicott Guardian in place, adherence to national guidelines).

Issue of consent and the use of patient-identifiable data: Justify why consent cannot or should not be obtained by either your organisation or the holder of the information you require.

Justify why data cannot be anonymised or pseudo-anonymised.

Show a clear commitment to making improvements in consent/anonymisation procedures wherever practicable.

Provide clear evidence that your organisation has made improvements in obtaining consent from patients since previous applications were submitted.

Provide details of why the purpose could not be satisfied in another reasonably practicable way (ie, without patient-identifiable data).

Benefit of the activity: Provide a clear and acceptable description of how the activity may improve patient care or be in the public interest.

Ethics approval: If the activity to be supported is research, gain appropriate ethics committee approval.

Security: Provide clear evidence that your organisation is following best practice in terms of IM&T [Information Management and Technology] security (eg, access controls, security policy, staff contracts, etc).

Where more than one organisation is seeking support, provide details showing that the lead/sponsor organisation has taken sufficient steps to ensure that the other organisations are maintaining the same IT security standards.¹⁸

should remember that section 60 is not a legal prerequisite for the use of patient-identifiable data in the absence of patient consent, since one can argue that the breach of confidentiality was covered by the common law public interest defence.

The Human Rights Act 1998

The HRA1998 will only be discussed briefly as it is assumed that compliance with the DPA1998 and the common law duty of confidentiality fulfil the requirements of the Act.¹ Article 8(1) of the HRA1998, provides that "Everyone has the right to respect for his private and family life, his home and his correspondence"; and that "the protection of personal data, not least medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life".²⁰

As with the law of confidentiality, the Article 8 right is not absolute. Article 8(2) provides that the interests of a patient and the community in protecting the confidentiality of medical information may be outweighed by other interests, such as the protection of health. The courts will undertake a balancing exercise in determining whether a disclosure of confidential information is in breach of Article 8, and it would seem that this process is little different from the balancing exercise that is performed when assessing whether a breach of confidentiality can be justified in the public interest. The monitoring and protection of public health through disease registers would

certainly fall within the protection of health specified in Article 8(2). It would then have to be shown that the use of confidential information without consent was both necessary and proportionate to that legitimate aim.

STOCKPORT CARDIOVASCULAR DISEASE REGISTER

Overview

The Stockport Cardiovascular Disease (CVD) Register was established as a pilot study in 2005 to explore the potential for epidemiological research into the incidence, aetiology and interventions to reduce the burden of CVD in Stockport. The register contains medical and demographic data for all Stockport residents diagnosed as having CVD since January 1998 to the present. Data on diagnoses, operations, medications, relevant test results, modifiable risk factors associated with CVD (eg, smoking status), comorbidities for diabetes and thyroid disease, and outcomes (date of death) are collected. To establish the whole patient-care pathway from diagnosis to treatment of CVD, all relevant primary, secondary and tertiary care centres, and national systems contribute data (fig 1).

Patient-identifiable data were required for creating patient care pathways and for epidemiological research. All records for each patient need to be identified and linked together, and duplicate records detected for deletion. Record linkage is only possible when all datasets share a unique patient identifier such as name or NHS number, and/or a collection of partial identifiers such as date of birth, gender and address.²¹ In reality, few datasets are 100% complete and accurate for a unique identifier—NHS number is typically incomplete and names are commonly misspelled. To ensure that records from the same individual are correctly matched, partial identifiers such as date of birth, gender and address are also required. A main research aim was to investigate inequalities in access to care. This is only possible with data on socioeconomic status (derived from postcode data), ethnicity, gender, geographical location and age.

Pursuing patient consent was deemed inappropriate owing to the methodological and financial concerns mentioned above—the cost associated with contacting over 30 000 individuals was deemed prohibitive.

Compliance with the law

To ethically and legally justify processing patient-identifiable data without patient consent, we embarked on a comprehen-

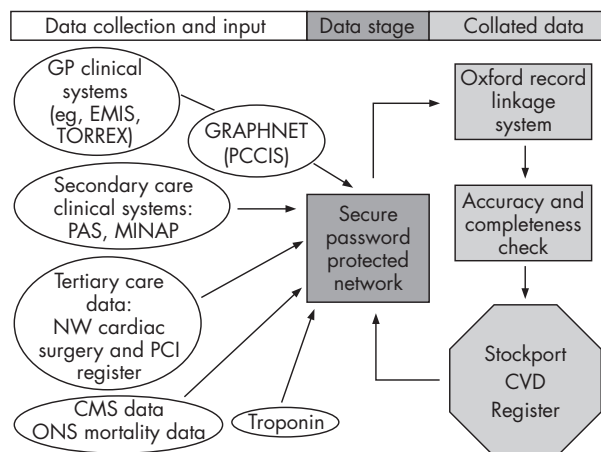


Figure 1 Data sources and data flow for the Stockport Cardiovascular Disease (CVD) Register. CMS, Commissioning Managing System; GP, general practitioner; MINAP, Myocardial Infarction Audit Project; ONS, Office for National Statistics; PAS, Patient Administration System; PCCIS, Patient Care Information Solutions; PCI, Percutaneous Coronary Intervention.

sive review of relevant ethical and legal guidelines. Our actions are discussed below with direct reference to the NHS Confidentiality Code of Conduct (fig 2).¹

Process 1: Caldicott principles of good practice

We ensured that the patient-identifiable data processed for the register complied with the Caldicott principles of good practice (table 1).²² To use the minimum necessary patient-identifiable data (Caldicott principle 3), we initially requested named data (first name and surname) as the principal identifier as validated record linkage programmes exist that primarily utilise named data.²¹ NHS number, date of birth, gender and address were also requested to ensure optimal record linkage—the more identifiers there are, the greater the likelihood of a correct match between records.^{21–23}

On completion of the record-linkage process, names and addresses would be encrypted, NHS numbers deleted and date

of birth replaced with age in years and days. The final linked dataset would retain age, gender, ethnicity and geographical output area (not postcode) for epidemiological research. Hence, the remaining patient-identifiable data would not allow the identification of an individual. These data items were approved by the Caldicott guardians.

Human Rights Act 1998

We have already discussed that the monitoring and protection of public health through disease registers falls within the “the protection of health” specified in Article 8(2). We could demonstrate that the use of confidential information without consent was necessary as there was no other way of compiling the register, and through complying with the NHS Code of Practice we showed that the use of such information was proportionate to the legitimate aim of establishing a disease register.

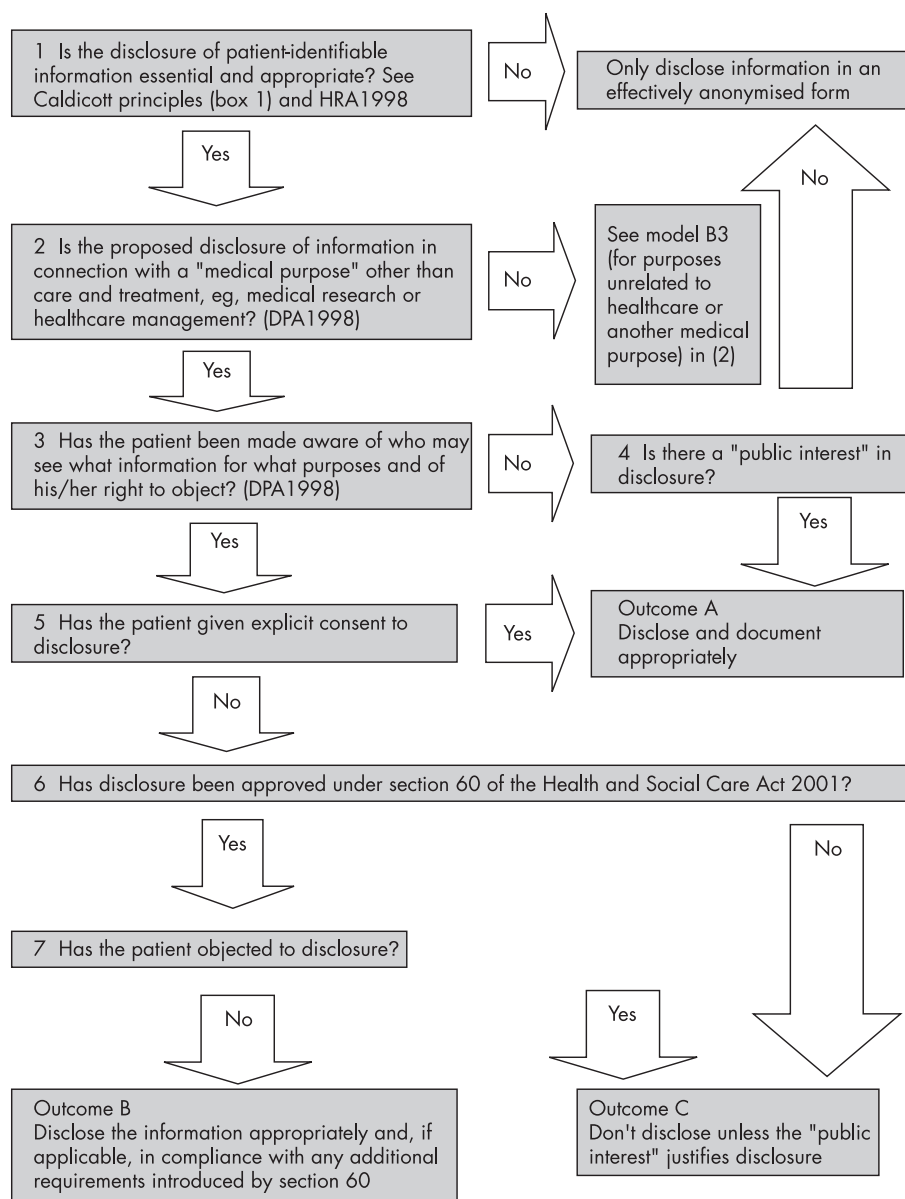


Figure 2 The National Health Service code of practice decision process involved in establishing whether it was acceptable to disclose confidential patient-identifiable data without patient consent for medical purposes; and what actions need to be taken to justify the disclosure of this information. DPA1998, Data Protection Act 1998; HRA1998, Human Rights Act 1998.

Process 2 and 3: DPA1998

To comply with the law for the use of patient-identifiable data (Caldicott principle 6), the register also had to comply with the DPA1998 (box 1). As the purpose of establishing the register was for medical research, it clearly adhered to Schedule 3 of the DPA1998, and the NHS Confidentiality Code of Conduct (process 2, fig 2). We could justify meeting Schedule 2 by claiming that the processing of data was necessary for research, which is a "legitimate interest", or we needed to show that the use of data would be in the public interest. For the CVD register, the reasoning that research would be in the public interest was a key issue and is discussed in further detail below.

The DPA98 also stipulates that when data controllers (eg, Stockport CVD Register "owners") have obtained personal data from someone other than the data subject (eg, from a general practitioner (GP)), they are exempt from the provision of fair processing when this would involve a "disproportionate effort". In relation to the register, the costs of obtaining consent for the use of retrospective data from all subjects were considered to be a disproportionate effort.

The DPA1998 does highlight the need for data subjects to "be fully aware of the ways in which their personal data may be processed in order for that processing to be considered fair".³ Public awareness of the register was ensured by sending each Stockport resident an information leaflet detailing how patient data may be used (process 3, fig 2) and how to object to the disclosure of information (process 7, fig 2). These leaflets are also available at General Practices and Stockport NHS Foundation Trust hospitals. The register was also advertised in national and local newsletters. No one to date has expressed a desire to have their data withdrawn from the register.

Although we felt that we could justify compliance with the Caldicott principles and DPA1998, the next step in the NHS Code of Practice decision process implied that approval under Section 60 of the Health and Social Care Act 2001 was required (process 6, fig 2). What did this entail and did we need it?

Process 4/outcome C: public interest?

The NHS Confidentiality Code of Conduct implies that if Section 60 approval is not sought, patient-identifiable data can nonetheless be collected without patient consent if they are to be used in the public interest (outcome C, fig 2). However, if someone decided to take the Stockport CVD Register owners or data contributors (eg, a GP supplying patient-identifiable data) to court for breach of the common law duty of confidentiality, we would have to convince a court that this was justified under the public interest defence.

The central issue, therefore, is what can be deemed as "in the public interest"? As previously mentioned, certain types of health research are likely to be deemed in the public interest. Therefore, organisations may be content to rely on compliance with the DPA98 and trust that if they were sued, the courts

would decide that their work is in the public interest. Alternatively, one may apply for Section 60 support.

Process 6: Section 60 of the Health and Social Care Act 2001

There was disagreement between the Acute Trust and Primary Care Trust Caldicott guardians as to whether Section 60 support was necessary. One Caldicott guardian was definite that support should be obtained. The other thought it was unnecessary as it is not absolutely essential from a legal stance. It was also viewed as difficult to obtain, and once applied for, if not granted, could result in termination of the whole project, or at best, considerable delay as PIAG convenes once every 3 months.

The register's steering group members did decide to apply for Section 60 support as this was regarded as best practice. There was also concern that GPs may be deterred from providing patients' data to the register because the common law duty of confidentiality is highlighted in guidelines from medical advisory groups on the disclosure of patient-identifiable data.²⁴⁻²⁷ This was an important consideration because populating the register relies on patient data from primary care, yet, GPs are under no obligation to provide such data.

Our initial application to PIAG for Section 60 support was rejected. PIAG believed that we had made insufficient efforts to identify alternatives to processing identifiable data. They recommended that we explore interrogation software to obtain anonymised data from GP systems. There was, however, no evidence that record linkage could be performed in the absence of patient identifiers from all data sources. We did find that accurate record linkage was possible using the NHS number as the unique identifier instead of names.²³ We relayed our findings to the PIAG secretariat, who informed us that the PIAG committee recognised the need for NHS numbers for record linkage. We also requested postcode, age, gender and ethnicity (which PIAG agreed to). PIAG also stated that it was essential that we consult patient/user groups before seeking Section 60 support in the future, which we did. With these amendments in place we secured Section 60 support on the second application. It took over 5 months from initial application to gaining Section 60 approval.

PIAG approval has been renewed for a second year owing to our ongoing efforts to involve users/patients in the register through membership on the steering group and an ethics and confidentiality advisory committee, local and national publications for the public, presentations at the local patient group for Stockport residents with CVD and our commitment to develop an exit strategy by seeking anonymised information in the future.

CONCLUSION

To disclose and collect patient-identifiable data without patient consent, for medical purposes other than healthcare, organisations must show that they comply with the

- DPA1998,
- HRA1998, and
- for NHS organisations and medical schools, the Caldicott principles of good practice.

Use of the NHS Code of Practice decision process described in fig 2 can be used as the basis for ensuring that processing of patient-identifiable data without patient consent follows best practice. The difficulty still remains when deciding on whether to apply for Section 60 support to protect against the common law duty of confidentiality. Organisations have been taken to court over breaches of the common law duty of confidentiality in the use of patient-identifiable data.¹⁶ Although it may be

Table 1 Caldicott general principles of good practice²¹

Principle 1	Justify the purpose for the use and transfer of each piece of patient-identifiable data
Principle 2	Don't use patient-identifiable information unless it is absolutely necessary for the specified purpose(s) of that flow
Principle 3	Use the absolute minimum necessary patient-identifiable information
Principle 4	Access to patient-identifiable information should be on a strict need-to-know basis
Principle 5	Everyone with access to patient-identifiable information should be aware of their responsibilities and obligations to respect patient confidentiality
Principle 6	Understand and comply with the law for the use of patient-identifiable data

unlikely that you are taken to court for a breach of the common law duty of confidentiality, owing to the unclear nature of what can be deemed as in the public interest, can you justify not applying for section 60 support?

Although it is not unlawful in itself to process patient-identifiable data without patient consent in the absence of Section 60 support, it does provide the most secure basis in law for processing such data. Current guidelines from the NHS,¹ General Medical Council,²⁵ British Medical Association²⁶ and Medical Research Council²⁷ also state that Section 60 support is a prerequisite before patient-identifiable data are disclosed without consent. Be aware that once an application for Section 60 support is made, it can result in considerable time delays and therefore costs, and in the worse case scenario, being told that consent is necessary.

ACKNOWLEDGEMENTS

We thank all members of the Stockport Cardiovascular (CVD) Register steering group for their contribution. We also thank Sarah O'Brien, Professor of Health Sciences & Epidemiology, Hope Hospital, and Dr Richard Phillips, Manchester Business School, for their comments on this manuscript. The Stockport CVD Register is funded by Stockport NHS Foundation Trust R&D.

Authors' affiliations

Charlotte L Haynes, Epidemiology, Stockport NHS Foundation Trust, Stepping Hill Hospital, Stockport, UK

Gary A Cook, Epidemiology, Stockport NHS Foundation Trust, Stepping Hill Hospital, Stockport, UK

Michael A Jones, Liverpool Law School, University of Liverpool, Liverpool, UK

Funding: This work was supported by Stockport NHS Foundation Trust R&D.

Competing interests: None.

REFERENCES

- 1 **Department of Health**. *Confidentiality: NHS Code of Conduct*, Version 3. London: DH, 2003, <http://www.dh.gov.uk/assetRoot/04/06/92/54/04069254.pdf> (accessed 27 July 2006).
- 2 **National Health Service**. NHS (Venereal Diseases) Regulations, SI 1974 Number 29. 1974.
- 3 **Information Commissioner's Office**. *Data Protection 1998, Legal Guidance*, Version 1. <http://www.informationcommissioner.gov.uk/cms/DocumentUploads/Data%20Protection%20Act%201998%20Legal%20Guidance.pdf> (accessed 27 July 2006).
- 4 **Strobl J**, Cave E, Walley T. Data protection legislation: interpretation and barriers to research. *BMJ* 2000;**321**:890–2.
- 5 **Al-Shahi R**, Warlow C. Using patient-identifiable data for observational research and audit. *BMJ* 2000;**321**:1031–2.
- 6 **Verity C**, Nicoll A. Consent, confidentiality, and the threat to public health Surveillance. *BMJ* 2002;**324**:1210–13.
- 7 **O'Brien J**, Chantler C. Confidentiality and the duties of care. *J Med Ethics* 2003;**29**:36–40.
- 8 **Iversen A**, Liddell K, Fear N, *et al*. Consent, confidentiality, and the Data Protection Act. *BMJ* 2006;**332**:165–9.
- 9 **Newton J**, Garner S. *Disease registers in England*. A report commissioned by the Department of Health Policy Research Programme in support of the White Paper entitled Saving lives: our healthier nation. Oxford: Institute of Health Sciences, 2002.
- 10 **Brown P**. Health bodies defend their right to access patient data. *BMJ* 2002;**324**:1236.
- 11 **Morrow J**. Data protection and patient's consent. *BMJ* 2001;**322**:549.
- 12 **Robling MR**, Hood K, Houston H, *et al*. Public attitudes towards the use of primary care patient record data in medical research without consent: a qualitative study. *J Med Ethics* 2004;**30**:104–9.
- 13 **Information Commissioner's Office**. Use and disclosure of health data. Guidance on the application of the Data Protection Act 1998. May, 2002.
- 14 **Wilson P**. Commentary: legal issues of data anonymisation in research. *BMJ* 2004;**328**:1300–1.
- 15 **Jones MA**. *Medical negligence*, 3rd edn. London: Sweet & Maxwell, 2003; (160–98).
- 16 R v Department of Health, ex parte Source Informatics QB 424 2001.
- 17 Health and Social Care Act 2001: s. 60(2) (c).
- 18 Application for section 60 support. <http://www.advisorybodies.doh.gov.uk/piag/applications.htm>.
- 19 **Turnberg L**. Common sense and common consent in communicable disease surveillance. *J Med Ethics* 2003;**29**:27–9.
- 20 Z v Finland (1998) 25 EHRR 371; (1997) 45 BMLR 107..
- 21 **Gill L**. OX-LINK: The oxford medical record linkage system. in *Record linkage techniques 1997*. Washington, DC: National Academy Press, 1999:15–33.
- 22 **Department of Health**. *Protecting and using patient information: A manual for Caldicott Guardians*. London: DH, 1999.
- 23 **Gill L**. Methodology and applications of building a national file of health and mortality data. *Aust J Stat* 2004;**33**:101–24.
- 24 Health Service (Control of Patient Information) Regulations 2002, SI 2002 No 1438, reg 4.
- 25 **General Medical Council**. *Confidentiality: protecting and providing information*. London, GMC, April 2004 <http://www.gmc-uk.org/guidance/library/confidentiality.asp>
- 26 **British Medical Association**. *Medical ethics today*, 2nd edn., London: BMA, October 2004.
- 27 **Medical Research Council**. *Personal information in medical research*. London: MRC, January, 2003.